

# TORSION GROUPS OF ELLIPTIC CURVES OVER QUADRATIC CYCLOTOMIC FIELDS IN ELEMENTARY ABELIAN 2-EXTENSIONS

ÖZLEM EJDER

ABSTRACT. Let  $K$  denote the quadratic field  $\mathbb{Q}(\sqrt{d})$  where  $d = -1$  or  $-3$ . Let  $E$  be an elliptic curve defined over  $K$ . In this paper, we analyze the torsion subgroups of  $E$  in the maximal elementary abelian 2-extension of  $K$ .

## 1. INTRODUCTION

Let  $E$  be an elliptic curve defined over the number field  $k$ . It is known by the Mordell-Weil theorem that the set  $E(k)$  of  $k$ -points on the elliptic curve  $E$  is a finitely generated abelian group and hence  $E(k)_{\text{tors}}$  is finite.

In 1977, Mazur classified the torsion subgroups of  $E(k)$  when  $k = \mathbb{Q}$ .

**Theorem 1** (Mazur). Let  $E$  be an elliptic curve defined over  $\mathbb{Q}$ . Then the torsion subgroup  $E(\mathbb{Q})_{\text{tors}}$  of  $E$  is isomorphic to one of the following groups:

$$\mathbb{Z}/N\mathbb{Z} \text{ for } 1 \leq N \leq 12, N \neq 11$$

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z} \text{ for } 1 \leq m \leq 4$$

The following theorem of Kenku, Momose, and Kamienny classified the torsion subgroups of  $E(k)$  when  $k$  is a quadratic number field.

**Theorem 2** (Kamienny, Kenku, and Momose). Let  $E$  be an elliptic curve defined over a quadratic field  $K$ . Then  $E(K)_{\text{tors}}$  of  $E(K)$  is isomorphic to one of the following groups:

$$\mathbb{Z}/m\mathbb{Z} \text{ for } 1 \leq m \leq 18, m \neq 17$$

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z} \text{ for } 1 \leq m \leq 6$$

$$\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3m\mathbb{Z} \text{ for } m = 1, 2$$

$$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}.$$

In this paper, we will be interested in the case where  $k$  is a quadratic cyclotomic field i.e,  $\mathbb{Q}(i)$  or  $\mathbb{Q}(\sqrt{-3})$ . The list of torsion subgroups of elliptic curves over the quadratic cyclotomic fields was recently determined by Filip Najman as given in the following theorem.

---

*Date:* February 2016.

**Theorem 3** (Najman).

- Let  $E$  be an elliptic curve defined over  $\mathbb{Q}(i)$ . Then  $E(K)_{\text{tors}}$  is one of the groups from Mazur's theorem or  $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ .
- Let  $E$  be an elliptic curve defined over  $\mathbb{Q}(\sqrt{-3})$ . Then  $E(K)_{\text{tors}}$  is one of the groups from Mazur's theorem,  $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$  or  $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ .

Let  $E$  be an elliptic curve defined over the number field  $k$  and  $F$  be the maximal elementary abelian two extension of  $k$  i.e,

$$F := k[\sqrt{d} : d \in \mathcal{O}_k]$$

Since  $F$  is not a number field,  $E(F)$  does not have to be finitely generated. Indeed, Frey and Jarden proved that it is not finitely generated but  $E(F)_{\text{tors}}$  is known to be finite and it is studied by Laska and Lorenz [9] and Fujita [2],[3] for the case when  $k = \mathbb{Q}$ . They have found 20 possible groups.

In this paper, we will generalize Laska-Lorenz and Fujita's work to the case where  $k$  is a quadratic cyclotomic field.

For the rest of the paper, let  $K$  denote the cyclotomic field  $\mathbb{Q}(i)$  or  $\mathbb{Q}(\sqrt{-3})$  and  $F$  is the maximal elementary abelian extension of  $K$ . By a  $K$ -rational subgroup we mean a  $\text{Gal}(\bar{K}/K)$  invariant subgroup of  $E(\bar{K})$ . We used the computer algebra system MAGMA for the computations.

## 2. ODD TORSION POINTS

Next result gives us a method of how to determine the odd torsion subgroup in an elementary abelian extension of  $k$ .

**Lemma 4** (Laska and Lorenz). Let  $E$  is an elliptic curve defined over the field  $k$  and  $L = k[\sqrt{d_i} \mid i = 1, \dots, n]$  be an elementary abelian two extension of  $k$ . Then

$$E(L)_{2'} \cong E^{(d_1)}(k)_{2'} \oplus \dots \oplus E^{(d_n)}(k)_{2'},$$

where  $E(k)_{2'} = \{P \in E(k) \mid nP = 0 \text{ for some odd } n\}$ . Furthermore, the image of each summand  $E^d(k)_{2'}$  is a  $k$ -rational subgroup of  $E(L)$ .

The following proposition will be useful for determining certain torsion subgroups of  $E(F)$ .

**Proposition 1.** Let  $E$  be an elliptic curve defined over  $K$ . Then  $E$  has no rational cyclic subgroup of order 24, 27, 32, 35, 36 or 45. Moreover, if  $E$  is defined over  $\mathbb{Q}(\sqrt{-3})$ , it does not have a rational cyclic subgroup of order 20, 21 and hence 63.

*Proof.* An elliptic curve  $E$  defined over  $K$  with a  $K$ -rational cyclic subgroup of order  $N$  corresponds to a non-cuspidal  $K$ -point on the modular curve  $X_0(N)$ . The computations of points on the corresponding curves (apart from 32) can be found in [14].

The elliptic curve  $y^2 = x^3 + 4x$  can be taken as a model for  $X_0(32)$ . This elliptic curve has only 4 points defined over  $\mathbb{Q}(\sqrt{-3})$  and 4 extra points over  $\mathbb{Q}(i)$ . All of these points are cusps. Hence there are no elliptic curves over  $K$  with a  $K$ -rational cyclic subgroup of order 32.  $\square$

**Remark.** The modular curve  $X_0(21)$  is an elliptic curve with Mordell-Weil rank 1 over  $K = \mathbb{Q}(i)$ . Hence  $X_0(21)$  is not very helpful for determining the possible order 21 subgroups of  $E(F)$ .

**Proposition 2.** Let  $E$  be an elliptic curve defined over  $\mathbb{Q}(i)$ . Then  $E(F)$  does not have a subgroup of order 21.

*Proof.* Let  $E$  be an elliptic curve defined over  $K = \mathbb{Q}(i)$  and suppose that  $E(F)$  has a subgroup of order 21. Then by Lemma 4, we may assume that  $E(K)$  has a point of order 7 and a point of order 3 defined over a quadratic extension of  $K$  (replacing by a twist if necessary). It can be found in [8] that elliptic curves with a point of order 7 can be parametrized as

$$E_t : y^2 + (1 - c)xy - by = x^3 - bx^2$$

where  $c = t^3 - t^2$  and  $b = t^2 - t$  for some  $t \neq 0, 1$  in  $K$ .

Therefore, we may assume  $E = E_s$  for some  $s \in K$  and the third division polynomial of the elliptic curve  $E_s$ :

$$\begin{aligned} \psi_3^s := x^4 + \left(\frac{1}{3}s^4 - 2s^3 + s^2 + \frac{2}{3}s + \frac{1}{3}\right)x^3 + (s^5 - 2s^4 + s^2)x^2 \\ + (s^6 - 2s^5 + s^4)x - \frac{1}{3}s^9 + s^8 - s^7 + \frac{1}{3}s^6. \end{aligned}$$

Remember that, by assumption,  $E$  has a point  $P$  of order 3 defined in a quadratic extension of  $K$ . Hence the subgroup generated by  $P$  is  $K$ -rational by Lemma 4 and it follows that the  $x$ -coordinate of the point  $P$  must be in  $K$  which forces  $\psi_3^s$  to have a root in  $K$ . Now,  $(E, P)$  corresponds to a point  $(s, x_0)$  on the curve  $C$  given by the equation

$$C : \psi_3^t(x) = 0$$

where  $E$  is isomorphic to  $E_s$  and  $x_0$  is the  $x$ -coordinate of the point  $P$  of order 3. Therefore it is enough to find  $C(K)$ , the set of  $K$ -points on  $C$ . The curve  $C$  is birational to a hyperelliptic curve

$$\tilde{C} : y^2 = f(x)$$

where

$$f(x) = x^8 - 6x^6 + 4x^5 + 11x^4 - 24x^3 + 22x^2 - 8x + 1.$$

$C$  and  $\tilde{C}$  are isomorphic over  $K$  outside the set of singularities which are  $\{(0, 0), (0, 1)\} \subset C$ . Hence it is enough to find  $\tilde{C}(K)$ . The polynomial  $f(x)$  factors as

$$f(x) = (x^2 - x + 1)(x^6 + x^5 - 6x^4 - 3x^3 + 14x^2 - 7x + 1)$$

Let  $g$  and  $h$  denote the factors of  $f$ :

$$g(x) = x^2 - x + 1$$

$$h(x) = x^6 + x^5 - 6x^4 - 3x^3 + 14x^2 - 7x + 1.$$

Using the Descent theorem ([19]), it is enough to find the points on the unramified coverings  $\tilde{C}_d$  of  $\tilde{C}$ , which are given as the intersection of two surfaces in  $\mathbb{A}^3$ :

$$w^2 = dg(x) = d(x^2 - x + 1)$$

and

$$y^2 = dh(x) = d(x^6 + x^5 - 6x^4 - 3x^3 + 14x^2 - 7x + 1)$$

where  $d$  is a square-free number in  $\mathcal{O}_K$  dividing the resultant of  $g(x)$  and  $h(x)$ , which is 112. Therefore  $d$  belongs to the set

$$\{1, i, (1+i), 7, i(1+i), 7(1+i), 7i, 7i(1+i)\}$$

For all the cases except  $d = 1$  and  $d = 7i$  we will look at the reduction of the covering at the primes extending 5 in  $\mathbb{Z}[i]$ . The curve

$$y^2 = d(x^6 + x^5 - 6x^4 - 3x^3 + 14x^2 - 7x + 1)$$

reduces to

$$y^2 = 2(x^6 + x^5 - 6x^4 - 3x^3 + 14x^2 - 7x + 1)$$

over  $\mathbb{F}_5$  and the second equation does not have any solutions over  $\mathbb{F}_5$ . Hence there are no  $K$ -rational points on  $\tilde{C}_d$  for  $d \neq 1, 7i$ . Let  $d = 7i$ . The Mordell-Weil rank of Jacobian of the curve

$$y^2 = d(x^6 + x^5 - 6x^4 - 3x^3 + 14x^2 - 7x + 1).$$

is zero and its torsion subgroup is identity over  $K$ . Therefore  $\tilde{C}_d(K) = \emptyset$  for  $d = 7i$ . (The points at infinity are not defined over  $K$ .)

Hence, if there is a point on the curve  $\tilde{C}(K)$ , it must be arising from the covering  $\tilde{C}_1(K)$ . Now the curve

$$C_2 : y^2 = x^6 + x^5 - 6x^4 - 3x^3 + 14x^2 - 7x + 1$$

is of genus two and  $\text{rank}(J(C_2)) = 2$ . Also  $J(C_2)_{\text{tors}} = \{1\}$ . This can be seen by reduction at good primes such as  $2 - i$  and  $3 - 2i$ . However,  $J(C_2)(\mathbb{Q})$  is also rank two and  $J(C_2)(\mathbb{Q}(i)) = J(C_2)(\mathbb{Q})$ . We claim that  $C_2(\mathbb{Q}) = C_2(\mathbb{Q}(i))$ .

Let  $J = J(C_2)$  and  $P$  be a point in  $C_2(K)$ . Let  $P_0$  denote the point  $[0 : 1 : 1]$  on  $C_2$ . Then  $[P - P_0]$  represents a point in  $J(K)$  which equals to  $J(\mathbb{Q})$ . If  $P'$  denotes the Galois conjugate of  $P$ , then  $[P' - P_0]$  must be equal to  $[P - P_0]$  since a point in  $J(\mathbb{Q})$  is  $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ -invariant. Hence  $P = P'$  and  $P$  is in  $C(\mathbb{Q})$ .

Now, we have proved that  $C_2(\mathbb{Q}) = C_2(\mathbb{Q}(i))$ . We claim that  $\tilde{C}(\mathbb{Q}) = \tilde{C}(\mathbb{Q}(i))$ . The first equation  $w^2 = x^2 - x + 1 = (x - 1/2)^2 + 3/4$  implies that if  $(a, b)$  is a point on  $C_1$  with  $a$  in  $\mathbb{Q}$ , then  $b$  is also in  $\mathbb{Q}$ . Hence  $\tilde{C}_1(K) = \tilde{C}_1(\mathbb{Q})$  and hence we proved the claim. This implies that a pair  $(E, P)$  on  $C(K)$  corresponds to a point  $(x, y)$  on  $\tilde{C}(\mathbb{Q})$ . However, if  $E$  is

defined over  $\mathbb{Q}$  and  $x(P) \in \mathbb{Q}$ , then  $P$  is in  $E(\mathbb{Q}(\sqrt{d}))$  for some  $d \in \mathbb{Q}$ . We know by [9] that  $E(F)$  does not have a subgroup of order 21 if the base field of  $E$  is  $\mathbb{Q}$ . Therefore there is no such curve  $E$  with a point of order 21 in a quadratic extension of  $K$ .  $\square$

**Proposition 3.** Let  $K$  be a quadratic cyclotomic field and  $E$  be an elliptic curve defined over  $K$ . Then  $E(F)_{2'}$  is isomorphic to one of the following groups:

$$\mathbb{Z}/N\mathbb{Z} \text{ for } N \in \{1, 3, 5, 7, 9, 15\} \text{ or } \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}.$$

*Proof.* By Lemma 4 and Theorem 3, we see that the odd numbers dividing the order of  $E(F)_{\text{tors}}$  are products of 3, 5, 7 and 9. Since  $F$  does not contain the fifth, seventh or ninth root of unity (odd number), by Weil pairing  $\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$ ,  $\mathbb{Z}/7\mathbb{Z} \oplus \mathbb{Z}/7\mathbb{Z}$  or  $\mathbb{Z}/9\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z}$  can not be isomorphic to a subgroup of  $E(F)$ . If  $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/7\mathbb{Z}$  or  $\mathbb{Z}/9\mathbb{Z} \oplus \mathbb{Z}/7\mathbb{Z}$  is a subgroup of  $E(F)$ , then it is Galois invariant by Lemma 4. Hence by Proposition 1 and Proposition 2, this is not possible. Similarly,  $\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/7\mathbb{Z}$  and  $\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z}$  are also not possible by Proposition 1.

If  $E(F)$  contains a subgroup isomorphic to  $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z}$ , then we may assume that  $E(K)$  has a point  $P$  of order 9 and has an additional rational subgroup  $C$  of order 3 (arising from a twist). Then by [13, Lemma 7],  $E$  is isogenous to an elliptic curve  $E'$  with a cyclic  $K$ -rational subgroup of order 27. There is no such curve by Proposition 1.

Finally,  $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$  can not be isomorphic to a subgroup of  $E(F)$  either. Otherwise,  $E(F)$  has a  $K$ -rational subgroup of order 15. By [13, Lemma 7] as above,  $E$  is isogenous to an elliptic curve with a cyclic  $K$ -rational subgroup of order 45 contradicting Proposition 1.  $\square$

### 3. THE MODULAR CURVE $X_0(64)$

An affine model for  $X_0(64)$  is given in Kenku's paper [6] as

$$x^4 + y^4 = 1.$$

Using this affine model, we first show that there are no elliptic curves defined over  $K$  with a rational cyclic subgroup of order 64. Kenku showed that there are four cusps defined exactly over  $\mathbb{Q}$  and four cusps exactly over  $\mathbb{Q}(i)$  and four extra cusps defined over the cyclotomic field of eight root of unity.

**Proposition 4.** The modular curve  $X_0(64)$  has no noncuspidal points over the cyclotomic fields  $K = \mathbb{Q}(i)$  or  $K = \mathbb{Q}(\sqrt{-3})$ .

*Proof.* Let  $(a, b)$  with  $(b \neq \pm 1)$  be solution to  $x^4 + y^4 = 1$ . Then  $u = 2a^2/(1 - b^2)$  and  $v = 4a/(1 - b^2)$  satisfy the equation  $v^2 = u^3 + 4u$ . The last equation is an affine model of an elliptic curve and it has 4 points over  $\mathbb{Q}(\sqrt{-3})$  and 8 points over  $\mathbb{Q}(i)$  (including the point at infinity).

Let  $K = \mathbb{Q}(\sqrt{-3})$ . Then  $(0, 0), (2, 4), (2, -4)$  are the only solutions to  $y^2 = x^3 + 4x$  over  $K$ . It is easy to see that the only solutions to  $(a, b)$  corresponding to these points are  $(\pm 1, 0)$  and when  $b = \pm 1$  we obtain the points  $(0, \pm 1)$ .

If  $K = \mathbb{Q}(i)$ , then we have four extra points on the elliptic curve namely,  $(2i, 0), (-2i, 0), (-2, 4i), (-2, -4i)$ . Similarly, we obtain the solutions  $a = 0, b = \pm i$  or  $\pm 1$  and  $a = \pm i, b = 0$ . We know that these points are cusps of  $X_0(64)$  by Kenku[6].  $\square$

The next lemma will be useful to prove that there are no quadratic points on  $X_0(64)(K)$  if  $K = \mathbb{Q}(i)$ . We will call a solution  $(x, y)$  of a Diophantine equation trivial if  $xy = 0$  and nontrivial otherwise.

**Lemma 5.** Let  $K = \mathbb{Q}(\sqrt{d})$  for  $d = -1$  or  $-3$ .

- The Diophantine equation  $x^4 + y^2 = 1$  has no nontrivial solutions over  $K$ .
- The Diophantine equation  $u^4 + v^4 = z^2$  has only trivial solutions over  $K = \mathbb{Q}(i)$ .

*Proof.*

- Let  $(a, b)$  be a solution of the given equation. Then similar to the previous proposition, we see that if  $b \neq 1$ ,  $u = 2a^2/(1 - b)$  and  $v = 4a/(1 - b)$  satisfy the equation  $v^2 = u^3 + 4u$ . Since we know the points on the elliptic curve  $v^2 = u^3 + 4u$ , analyzing the inverse images of these points we find that the solutions are  $(\pm 1, 0), (0, \pm 1)$  over  $\mathbb{Q}(\sqrt{-3})$  and two more points  $(\pm i, 0)$  over  $\mathbb{Q}(i)$ .
- If  $(a, b, c)$  is a solution in  $K$  to the given equation. Then  $(2a^2/(b^2 - c), 4ab/(b^2 - c))$  is a solution to the equation  $y^2 = x^3 - 4x$ . It has only three points  $(0, 0), (2i, 0), (-2i, 0)$  over  $K$  and computing  $a, b, c$  corresponding to these points and the points where  $b^2 = c$ , we see that  $abc = 0$  in all cases.

$\square$

**Theorem 6.** Let  $K = \mathbb{Q}(i)$ . Then only nontrivial solutions to the equation  $x^4 + y^4 = 1$  are defined over the quadratic extension  $L = K(\sqrt{-7})$ .

*Proof.* We will follow Mordell's idea ([11, Chapter 14, Theorem 4]) for the proof of this theorem. Let  $L$  be a quadratic extension of  $K$  and  $(a, b)$  be a solution in  $L$ . We can find a  $t \in L$  such that  $a^2 = 1 - t^2/(1 + t^2), b^2 = 2t/(1 + t^2)$ . We will analyze the equation in two cases:  $t$  is in  $K$  or  $t$  is not in  $K$ . Let  $t$  be in  $K$ . If either  $a$  or  $b$  is in  $K$ , then  $(a, b^2)$  or  $(a^2, b)$  gives a solution to the equation  $x^4 + y^2 = 1$  (respectively  $x^2 + y^4 = 1$ ) which are trivial by the first part of Lemma 5.

If neither  $x$  nor  $y$  is in  $K$ , then  $x = x_1\sqrt{w}$  and  $y = y_1\sqrt{w}$  for some  $x_1, y_1$  in  $K$  since  $x^2, y^2 \in K$ . Hence  $(x_1, y_1, 1/w)$  is a solution to  $x^4 + y^4 = z^2$ . By the second part of Lemma 5, this is not possible.

Assume  $t \notin K$ . Since  $a, b$  are in  $L$ ,  $K(t)$  is a quadratic extension of  $K$  and hence equals to  $L$ . Let  $F(t)$  be the minimal polynomial of  $t$  over  $K$  and let us define  $X, Y$  as follows:

$$X = (1 + t^2)xy, \quad Y = (1 + t^2)y$$

Then, it is easy to see that  $X^2 = 2t(1 + t^2)$  and  $Y^2 = 2t(1 - t^2)$ . Since  $X, Y$  are in  $L$ , then there are  $c, d, e, f \in K$  such that

$$X = c + dt, \quad Y = e + ft$$

Then  $t$  satisfies the equations

$$g(z) = (c + dz)^2 - 2z(1 - z^2) = 0, \quad (h(z) = (e + fz)^2 - 2z(1 + z^2) = 0.$$

Since  $F(z)$  is the minimal polynomial of  $t$  over  $K$ ,  $F(z)$  divides  $g$  and  $h$  and so  $g$  and  $h$  both have exactly one root over  $K$  (not necessarily the same root). Let us call these roots  $u, v$  respectively.

Then  $(-2u, 2(c + du))$  satisfies  $y^2 = x^3 - 4x$ . Since this is an affine model of an elliptic curve, we can easily compute the points on it. There are three of them; namely,  $(0, 0), (2, 0), (-2, 0)$ . Notice that  $(2v, 2(e + fv))$  is a point on the curve  $y^2 = x^3 + 4x$ . Hence computing the points on this curve, we see that only possible solutions for  $(2v, 2(e + fv))$  are  $(0, 0), (2i, 0), (-2i, 0), (2, 4), (2, -4), (-2, 4i), (-2, -4i)$ . We will compute the characteristic polynomial of  $t$  for each case and compare the coefficients.

The point  $(0, 0)$  on  $E$  corresponds to the solution  $z = 0$  and the equation  $g(z) = 0$  becomes  $d^2z^2 - 2z(1 - z^2) = 0$ . Cancelling the  $z$  factor and dividing by the leading coefficient, we find in this case that

$$F(z) = z^2 + d^2/2z - 1 \tag{1}$$

The point  $(2, 0)$  corresponds to the solution  $z = 1$  and the equation becomes  $d^2(1 - z)^2 - 2z(1 - z^2) = 0$ . Cancelling the  $(z - 1)$  term, and dividing by the leading coefficient, we find that

$$F(z) = z^2 + z(1 + d^2/2) - d^2/2 \tag{2}$$

Similarly, the point  $(-2, 0)$  gives us the solution  $z = -1$ . The equation becomes  $d^2(1 + z)^2 - 2z(1 - z^2) = 0$ . Dividing by  $(z + 1)$  and the leading coefficient, we obtain

$$F(z) = z^2 + z(-1 + d^2/2) + d^2/2 \tag{3}$$

Now, we will check the cases for the second equation  $h(z) = 0$ .

In a similar way, it is easy to compute the characteristic polynomial of  $t$  for the points  $(0, 0), (2i, 0)$  and  $(-2i, 0)$ . For the point  $(0, 0)$ , we have

$$F(z) = z^2 - \left(\frac{f^2}{2}\right)z + 1 \tag{i}$$

For  $(2i, 0)$ ,

$$F(z) = z^2 + \left(\frac{i - f^2}{2}\right)z + \frac{if^2}{2} \tag{ii}$$

and for  $(-2i, 0)$ ,

$$F(z) = z^2 + \left(\frac{-i - f^2}{2}\right)z - \frac{if^2}{2}. \quad (\text{iii})$$

We still need to check the points  $(2, 4), (2, -4), (-2, 4i)$  and  $(-2, -4i)$ . For these points, we will apply the same method to find  $F(z)$  but we will also have to do long division. Here is what we find for the point  $(2, -4)$ ,

$$F(z) = z^2 - \frac{(f^2 - 2)}{2}z + \frac{(f + 2)^2}{2} \quad (\text{iv})$$

and for  $(2, 4)$ , the characteristic polynomial,

$$F(z) = z^2 - \frac{(f^2 - 2)}{2}z + \frac{(f - 2)^2}{2} \quad (\text{v})$$

For  $(-2, 4i)$ ,

$$F(z) = z^2 - \frac{(f^2 + 2)}{2}z - \frac{(f + 2i)^2}{2} \quad (\text{vi})$$

Finally for  $(-2, -4i)$ , we have

$$F(z) = z^2 - \frac{(f^2 + 2)}{2}z - \frac{(f - 2i)^2}{2} \quad (\text{vii})$$

The polynomial in (1) is not possible since either the constant coefficients do not match or  $\pm 2, \pm i$  has to have a square root in  $K$ . The polynomial in (2) can not be equal to (i), (ii) or (iii) since 2 or  $-i$  is not a square in  $K$ . If we compare the polynomial in (2) to the ones in (iv,v,vi,vii), we obtain the polynomials

$$F(z) = z^2 + (1/2)z + 1/2, \quad F(z) = z^2 - z + 2.$$

For the same reason, the polynomial in (3) can not be equal to i,ii or iii. If (3) happens with (iv) or (v) then  $f = -2, 0$  or  $f = 0, 2$ . Also (3) and (vi) or (vii) gives us  $f = -i, i$ . The solutions  $f = 0$  and  $f = \pm i$  produces

$$F(z) = z^2 + z + 2, \quad F(z) = z^2 - (1/2)z + 1/2.$$

Now, one can check that splitting fields of these four polynomials over  $K$  are all the same field; namely  $K(\sqrt{-7})$ . After computing possible  $t$  values and  $a^2, b^2$ , we conclude that the solutions to the equation  $x^4 + y^4 = 1$  are obtained by multiplying the coordinates of the points  $(\frac{1+w}{2}, \frac{1-w}{2})$  and  $(1, 0)$  by  $\pm 1$  or  $\pm i$  and interchanging the coordinates where  $w$  is square root of  $-7$ . □

**Remark.** The same result over the field  $K = \mathbb{Q}(\sqrt{-3})$  does not hold since there are non-trivial  $K$ -solutions to the equation  $u^4 + v^4 = z^2$ .

**Proposition 5.** Let  $E$  be an elliptic curve defined over  $\mathbb{Q}(i)$ . Assume  $E$  has a cyclic isogeny of degree 64 defined over a quadratic extension of  $\mathbb{Q}(i)$ , then the  $j$ -invariant of  $E$  is integral.



*Proof.* We described the cuspidal points on  $X_0(64)$  in the beginning of the section. The  $j$ -invariants of the elliptic curves corresponding to the points defined over  $\mathbb{Q}(\sqrt{-7})$  are integral by the result of Kenku(1975). Thus, we only need to compute the  $j$ -invariants of the elliptic curves corresponding to the points defined over  $\mathbb{Q}(i, \sqrt{-7})$  but not in a quadratic extension of  $\mathbb{Q}$  that we found in the previous theorem. Magma computes that each of these 32 points produces an elliptic curve with an integral  $j$ -invariant.  $\square$

**Remark.** Over  $K = \mathbb{Q}(\sqrt{-3})$ , we find a point  $(2/\sqrt{5}, \sqrt{-3}/\sqrt{5})$  on the curve  $x^4 + y^4 = 1$  and a computation on magma shows that it produces an elliptic curve with a non-integral  $j$ -invariant.

**Lemma 7.** Let  $E$  be an elliptic curve over  $\mathbb{Q}(i)$  and  $F$  be the maximal elementary abelian two extension of  $\mathbb{Q}(i)$ . Then  $E(F)$  can not have a  $K$ -rational cyclic subgroup of order 20.

*Proof.* The modular curve  $X_0(20)$  has genus 1 and  $y^2 = x^3 + x^2 + 4x + 4$  can be taken as a model. This elliptic curve has Mordell-Weil group isomorphic to  $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$  over  $\mathbb{Q}(i)$ . It is known that six of these points are rational and these correspond to cusps. Remaining points are

$$\{(\pm 2i, 0), (2i - 2, \pm(2i + 4)), (-2i - 2, \pm(2i - 4))\}$$

The first four points corresponds to four isomorphic (over  $\bar{\mathbb{Q}}$ ) elliptic curves with a  $j$ -invariant 287496. Let us call  $E$  as any of these corresponding curves. They all have good reduction at prime 3 and 16 points over  $\mathbb{F}_9$  and reach up to 64 points over  $\mathbb{F}_{81}$ . Since there exist a unique quadratic extension of  $\mathbb{F}_9$ , if  $E(F)$  has a subgroup of order 20, then 20 should divide  $E(\mathbb{F}_{81})$  which is a contradiction. For the remaining two points,  $j$ -invariant is either 0 or 1728.

In this case, an elliptic curve with  $j$ -invariant 0 or 1728 can not have a point of order 5 by [14, Theorem 3.2.2]. Therefore if this curve has a subgroup of order 20 over  $F$ , (replacing by a quadratic twist if necessary) we may assume that it has a point of order 5 over  $\mathbb{Q}(i)$  which is not possible.  $\square$

**Proposition 6.** Let  $K = \mathbb{Q}(\sqrt{d})$  for  $d = -1$  or  $-3$  and  $F$  be the maximal elementary abelian extension of  $K$ . Assume that  $E$  is an elliptic curve defined over  $K$ .

- If  $K = \mathbb{Q}(i)$ , then  $E(F)$  does not contain a rational subgroup isomorphic to one of the following groups:

$$\begin{aligned} &\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}, \quad \mathbb{Z}/32\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \\ &\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}, \quad \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}. \end{aligned}$$

- If  $K = \mathbb{Q}(\sqrt{-3})$ . Then  $E(F)$  does not contain a rational subgroup isomorphic to the group

$$\begin{aligned} &\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}, \quad \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \\ &\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}. \end{aligned}$$

*Proof.* The proof follows from Proof of Proposition 2.4 in [9] using Proposition 5, Proposition 1 and Lemma 7.  $\square$

**Theorem 8.** Let  $K$  be a quadratic cyclotomic field and  $F$  be the maximal elementary abelian extension of  $K$ . Assume that  $E$  is an elliptic curve defined over  $K$ .

- If  $K = \mathbb{Q}(i)$ , then  $E(F)_{\text{tors}}$  is isomorphic to one of the following groups:

$$\mathbb{Z}/2^{b+r}\mathbb{Z} \oplus \mathbb{Z}/2^b\mathbb{Z} \quad (b = 1, 2, 3 \text{ and } r = 0, 1, 2, 3)$$

$$\mathbb{Z}/2^{b+r}\mathbb{Z} \oplus \mathbb{Z}/2^b\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \quad (b = 1, 2, 3 \text{ and } r = 0, 1)$$

$$\mathbb{Z}/2^b\mathbb{Z} \oplus \mathbb{Z}/2^b\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \quad (b = 1, 2, 3)$$

$$\mathbb{Z}/2^b\mathbb{Z} \oplus \mathbb{Z}/2^b\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z} \quad (b = 1, 2, 3)$$

or  $1, \mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/5\mathbb{Z}, \mathbb{Z}/7\mathbb{Z}, \mathbb{Z}/9\mathbb{Z}, \mathbb{Z}/15\mathbb{Z}$ , and  $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ .

- If  $K = \mathbb{Q}(\sqrt{-3})$ , then  $E(F)$  is either isomorphic to one of the above groups or

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/32\mathbb{Z}, \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/64\mathbb{Z}$$

*Proof.* Proof follows from [9, Proof of Theorem 2.5] using Proposition 6, Proposition 1, Lemma 7, Proposition 3 and Theorem 3.  $\square$

#### 4. $E(K)$ HAS FULL 2-TORSION

We know that the points of order 2 on  $E$  are given by the roots of the polynomial  $f(x)$  where  $E : y^2 = f(x)$ . Therefore, we may assume  $E$  is of the form  $y^2 = (x - \alpha)(x - \beta)(x - \gamma)$ . We will need the following results and use them very often in this section. Remember that  $F$  denotes the maximal elementary abelian extension of  $K$ .

**Lemma 9** (Knapp). [7] Let  $k$  be a field of characteristic not equal to 2 or 3, and  $E$  an elliptic curve over  $k$  given by  $y^2 = (x - \alpha)(x - \beta)(x - \gamma)$  with  $\alpha, \beta, \gamma$  in  $k$ . For  $P = (x, y)$  in  $E(k)$ , there exists a  $k$ -rational point  $Q$  on  $E$  such that  $[2]Q = P$  if and only if  $x - \alpha, x - \beta$  and  $x - \gamma$  are all squares in  $k$ . Furthermore, in this case if we fix the sign of the square roots of  $x - \alpha, x - \beta, x - \gamma$ , then the  $x$ -coordinate of  $Q$  equals to one of the following:

$$\sqrt{x - \alpha}\sqrt{x - \beta} \pm \sqrt{x - \alpha}\sqrt{x - \gamma} \pm \sqrt{x - \beta}\sqrt{x - \gamma} + x$$

**Theorem 10** (Ono). [16] Let  $K$  be a number field and  $E/K$  an elliptic curve with full 2-torsion. Then  $E$  has a model of the form  $y^2 = x(x + M)(x + N)$  where  $M, N \in \mathcal{O}_K$ .

- $E(K)$  has a point of order 4 iff  $M, N$  are both squares (in  $\mathcal{O}_K$ ) or  $-M, N - M$  are both squares or  $-N, M - N$  are both squares.
- $E(K)$  has a point of order 8 iff there exists a  $d \in \mathcal{O}_K$ ,  $d \neq 0$  and a Pythagorean triple  $(u, v, w)$  such that  $M = d^2u^4$ ,  $N = d^2v^4$ , or we can replace  $M, N$  by  $-M, N - M$  or  $-N, M - N$  as in the first case.

By Theorem 10, we may assume that an elliptic curve  $E$  with full 2-torsion has the model  $y^2 = x(x+a)(x+b)$  and furthermore, if  $E$  has a point of order 4 in  $E(F)$ , we may assume that there is a point  $Q$  such that  $[2]Q = (0, 0)$  and so  $a$  and  $b$  are squares. If  $E$  is given as  $y^2 = x(x+a)(x+b)$ , then the quadratic twist of  $E$  by  $d$  is given by  $E^d : y^2 = x(x+da)(x+db)$ . The elliptic curves  $E$  and  $E^d$  are isomorphic over a quadratic extension of  $K$  and the isomorphism is given by  $(x, y) \mapsto (dx, y\sqrt{d})$ . Before we start analyzing each case, we will state a result on classification of twists of elliptic curves over  $K$ .

**Theorem 11** (Newman). [14] Let  $K = \mathbb{Q}(\sqrt{D})$ ,  $D = -1, -3$  with  $d \in K$  a non-square, and  $E/K$  an elliptic curve with full 2-torsion. Then,

- If  $E(K)_{\text{tor}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ , then  $E^d(K)_{\text{tor}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ .
- If  $E(K)_{\text{tor}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ , then  $E^d(K)_{\text{tor}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ .
- If  $E(K)_{\text{tor}} \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ , then  $K = \mathbb{Q}(i)$  and  $E^d(K)_{\text{tor}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ .
- If  $E(K)_{\text{tor}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ , then  $E^d(K)_{\text{tor}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$  unless  $K = \mathbb{Q}(\sqrt{-3})$  and  $d = -1$  in which case  $E^d(K)_{\text{tor}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$  or  $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ .
- If  $E(K)_{\text{tor}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ , then  $E^d(K)_{\text{tor}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$  for almost all  $d$ .

In the rest of the paper,  $[n]$  denotes multiplication by  $n$  on the elliptic curve  $E$ .

**Proposition 7.** Let  $E : y^2 = x(x+a)(x+b)$  be an elliptic curve defined over  $K$ . Assume that  $E(K)_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ . Then

- If  $K = \mathbb{Q}(i)$ , then  $E(F)_{\text{tors}}$  is either isomorphic to  $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}$  or  $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/32\mathbb{Z}$ .
- If  $K = \mathbb{Q}(\sqrt{-3})$ , then  $E(F)$  is isomorphic to one of the groups above or  $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/64\mathbb{Z}$ .

*Proof.* Since any number in  $K$  is a square in  $F$ ,  $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z} \subset E(F)$  by Lemma 9. By Theorem 10, we may assume that  $a = u^4$  and  $b = v^4$  for some  $u, v \in \mathcal{O}_K$  such that  $u^2 + v^2 = w^2$  for some  $w \in K$ . We will show that  $\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z} \not\subset E(F)$ . Let  $Q_2 = (x, y)$  be a point of order 4 such that  $[2]Q_2 = (-a, 0)$ . By Lemma 9, we compute that  $x$  equals to one of the followings:

$$\pm \sqrt{-u^4 + 0} \sqrt{-u^4 + v^4} - u^4.$$

If  $\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z} \subset E(F)$ , then there is a point  $Q_3$  in  $E(F)$  such that  $[2]Q_3 = Q_2$  and by Lemma 9,  $x + u^4$  is a square in  $F$ . Hence  $x + u^4 = \pm \sqrt{-u^4} \sqrt{(-u^4 + v^4)} = \pm u^2 \sqrt{u^4 - v^4}$  is a square in  $F$ . Since  $u^2$  and  $-u^2 = (iu)^2$  are both squares in  $F$ , we need to analyze if  $\sqrt{u^4 - v^4}$  is a square in  $F$  or not. we will need the lemma below.

**Lemma 12.** Let  $\alpha$  be in  $K$ . If  $\sqrt{\alpha}$  is a square in  $F$ , then  $\alpha$  or  $-\alpha$  is a square in  $K$ . If  $K = \mathbb{Q}(i)$ , then  $\alpha$  must be a square in  $K$ .

*Proof.* Let  $w \in F$  be such that  $w^2 = \sqrt{\alpha}$ . Then  $w$  is a root of the polynomial  $f(x) = x^4 - \alpha$  defined over  $K$ . Since  $f$  has one root in  $F$  and  $F$  is a Galois extension of  $K$ ,  $f$  splits in  $F$ . If  $f$  is reducible over  $K$ , then it has to be product of two quadratic polynomials, otherwise 3 has to divide the order of  $\text{Gal}(F/K)$ . Let us write  $f$  as a product of two polynomials.

$$x^4 - \alpha = (x^2 + ex + f)(x^2 + cx + d)$$

Then  $ec + f + d = 0$ ,  $ed + fc = 0$  and  $c + e = 0$ . Therefore, replacing  $e$  by  $-c$ , we obtain  $c(f - d) = 0$ . So, either  $c = 0$  or  $f = d$ . If  $c = 0$ , then  $f = -d$  and so  $fd = -\alpha$  implies that  $\alpha = f^2$  in  $K$ . If  $f = d$ , then  $\alpha = -fd$ , so  $-\alpha$  is a square in  $K$ . Now, assume that  $f$  is irreducible over  $K$ . Then Galois group of  $f$  over  $K$  is an elementary abelian 2 group as a quotient of  $\text{Gal}(F/K)$ . Only elementary abelian 2-subgroups of  $S_4$  are order 2 or Klein four group  $V_2$ , so it must be  $V_2$ . If  $f$  remains irreducible in  $K(i)$ , we obtain an automorphism of order 4 in  $\text{Gal}(K(w)/K(i))$ ; namely  $w \mapsto iw$  which contradicts the fact that Galois group is  $V_2$ . Therefore, if  $K = \mathbb{Q}(i)$ , it can not be irreducible. Hence let  $K = \mathbb{Q}(\sqrt{-3})$ . Then  $f$  has to be reducible over  $K(i)$  and by the argument given above, we see that  $\alpha$  or  $-\alpha$  is a square in  $K(i)$ . Hence if  $\alpha = \pm d^2$  with  $d \in K(i)$ , then  $d = bi$  for some  $b \in K$  and  $\alpha = \pm b^2$ . □

By Lemma 12, we see that  $u^4 - v^4$  or  $v^4 - u^4$  has to be a square in  $K$ . Therefore  $(u, v, t)$  or  $(v, u, t)$  satisfy the equation  $x^4 - y^4 = z^2$  for some  $t \in K$ . However,

**Lemma 13.** Let  $K$  be  $\mathbb{Q}(\zeta_n)$  for  $n = 3$  or  $8$ . If  $(x, y, z)$  is a solution to the equation  $x^4 - y^4 = z^2$  over  $K$ , then  $xyz = 0$ .

*Proof.*  $(\frac{2y^2}{(x^2-z)}, \frac{4xy}{(x^2-z)})$  is a solution to  $y^2 = x^3 + 4x$ . Let  $E$  denote the elliptic curve  $y^2 = x^3 + 4x$ . Then  $E(\mathbb{Q}(i)) = \{(0, 0), (\pm 2i, 0), (2, \pm 4), (-2, \pm 2i), O\}$  and  $E(\mathbb{Q}(\zeta_8))$  attains these extra points

$$\begin{aligned} &(2\zeta_8^3 + 2\zeta_8^2 + 2\zeta_8, \pm(-4\zeta_8^3 - 4\zeta_8^2 + 4)), \\ &(2\zeta_8^3 - 2\zeta_8^2 + 2\zeta_8, \pm(4\zeta_8^3 - 4\zeta_8^2 + 4)), \\ &(-2\zeta_8^3 + 2\zeta_8^2 - 2\zeta_8, \pm(-4\zeta_8^3 + 4\zeta_8^2 - 4)), \\ &(-2\zeta_8^3 - 2\zeta_8^2 - 2\zeta_8, \pm(4\zeta_8^3 + 4\zeta_8^2 + 4)). \end{aligned}$$

where  $\zeta_8$  denotes a primitive 8'th root of unity. Also  $E(\mathbb{Q}(\sqrt{-3}))$  equals to  $E(\mathbb{Q})$  and it is contained in  $E(\mathbb{Q}(i))$ . Hence it is enough to look at inverse images of points in  $E(\mathbb{Q}(\zeta_8))$ . For all points in  $E(\mathbb{Q}(\zeta_8))$ , we simply compute the quotient of the first and the second coordinate of every point given above and find that  $xyz = 0$ . □

Notice that  $u$  or  $v$  can not be zero since  $E$  is non-singular. So, by Lemma 13,  $u^4$  must equal to  $v^4$  which means  $a$  equals to  $b$  which also leads to a singularity. Hence we have showed that  $E(F)$  does not contain a subgroup isomorphic to  $\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ . Theorem 11 implies that  $E(F)_{2'} = 0$ . Hence the result follows from Theorem 8.  $\square$

**Proposition 8.** Assume  $E(K)_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ . Then  $E(F)_{\text{tors}}$  is isomorphic to  $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$ .

*Proof.* All of the quadratic twists of  $E$  have torsion subgroup isomorphic to  $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$  by Theorem 11. Hence the odd part of  $E(F)_{\text{tors}}$  must be isomorphic to  $\mathbb{Z}/3\mathbb{Z}$ . By Lemma 9, we know that  $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \subset E(F)$  since  $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \subset E(K)$ .

We need to check if there is a point of order 8 in  $E(F)$ . Let  $P_2$  be in  $E(F)$  such that  $[2]P_2 = P_1 = (0, 0)$ . We compute the  $x$ -coordinate of  $P_2$  by Lemma 9 as

$$x(P_2) = \pm\sqrt{ab}.$$

Then  $P_2$  is either  $(\sqrt{ab}, \pm\sqrt{ab}(\sqrt{a} + \sqrt{b}))$  or  $(-\sqrt{ab}, \pm\sqrt{ab}(-\sqrt{a} + \sqrt{b}))$ . If  $P_2$  is in  $[2]E(F)$ , then again by Lemma 9,  $\sqrt{ab}$  has to be a square in  $F$  and by Lemma 12,  $ab$  or  $-ab$  is a square in  $K$ . We may assume that greatest common divisor of  $a, b$  is square-free. Otherwise we can replace  $E$  by the quadraic twist of  $E$  by  $d^2$  where  $d^2/(a, b)$ . Now let  $ab$  be a square in  $K$ . Then  $a = da'^2$  and  $b = db'^2$  where  $(a', b')$  is a unit.

Then

$$P_2 = (\pm da'b', da'b'(\pm a'\sqrt{d} + b'\sqrt{d}))$$

and the point

$$(\pm da'b', da'b'(\pm a' + b'))$$

defines a point of order 4 in  $E^d(K)$ . This contradicts that any quadratic twist of  $E$  has torsion group isomorphic to  $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$  over  $K$ . Hence  $ab$  is a square. Let  $a = da'^2$  and  $b = -db'^2$ . If  $P_2$  is in  $[2]E(F)$ , then  $x(P_2) + a$  is a square in  $F$ .

$$x(P_2) + a = \pm\sqrt{ab} + a = (da'b')i + da'^2 = da'(a' + b'i)$$

Hence  $a' + b'i = u^2s$  for some  $u$  in  $K(i)$  and  $s \in K$ . We also see that  $a' - b'i = \bar{u}^2s$  where  $\bar{u}$  denotes the Galois conjugate of  $u$ . Then  $a'^2 + b'^2 = (u\bar{u})^2s^2$  is a square in  $K$ . Now, consider the curve  $E' : y^2 = x(x + a - b)(x - b)$  which is isomorphic to  $E$  by the map taking  $x$  to  $x + b$ . Taking the quadratic twist of  $E'$  by  $d$ , we obtain  $E'^d : y^2 = x(x + d(a - b)(x - db))$ . Notice that  $d(a - b) = d^2(a'^2 + b'^2)$  and  $-db = d^2b'^2$ . Hence  $E'^d$  has to have a point of order 4 by Lemma 9 which is not possible by Theorem 11 since  $E$  and  $E'$  are isomorphic over  $K$ . Hence  $P_2$  is not in  $[2]E(F)$ .

The elliptic curve  $E' : y^2 = x(x - a)(x + b - a)$  is isomorphic to  $E : y^2 = x(x + a)(x + b)$  by the map taking  $(x, y)$  to  $(x - a, y)$  over  $K$ . Hence we proved above that there is no point  $P$  of order 8 in  $E'(F)$  such that  $[4]P = (0, 0)$ . Since the isomorphism between  $E$  and  $E'$  carries the point  $(0, 0)$  to  $(-a, 0)$ ,

there is no point  $Q$  in  $E(F)$  such that  $[4]Q = (-a, 0)$ . A similar argument can be done for  $(-b, 0)$ .

Therefore, there is no point of order 8 in  $E(F)$ . This proves that  $E(F) \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ .  $\square$

**Proposition 9.** Assume that  $E(K)_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ . Then,

- Let  $K = \mathbb{Q}(i)$ . Then  $E(F)$  does not contain a subgroup isomorphic to  $\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ .
- Let  $K = \mathbb{Q}(\sqrt{-3})$ . Then  $E(F) \cong \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$  if  $E^{(-1)}(K)$  has a point of order 4. Otherwise,  $E(F)$  does not contain a subgroup isomorphic to  $\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ .

*Proof.* By Lemma 9, we know that  $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z} \subset E(F)$ . We first determine if  $E(F)$  has a subgroup isomorphic to  $\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ . By Theorem 10, we may assume that  $a = s^2$  and  $b = t^2$  for some  $s, t \in \mathcal{O}_K$  relatively prime. Assume  $\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z} \subset E(F)$ .

Let  $Q_1 = (-s^2, 0)$  and  $Q_2$  be in  $E(F)$  so that  $[2]Q_2 = Q_1$ . Then by Lemma 9,  $x(Q_2) + s^2$  is a square in  $F$ . Computing  $x(Q_2)$ , we see that  $s\sqrt{s^2 - t^2}$  is a square in  $F$ . So,  $\sqrt{s^2 - t^2}$  is a square in  $F$  and by Lemma 12,  $\pm(s^2 - t^2)$  is a square in  $K$ . Let  $s^2 - t^2 = r^2$  for  $r \in K$ , then

$$Q_2 = (\pm sr, isr(r \pm s)).$$

Similarly, let  $R_2$  be a point such that  $[2]R_2 = (-t^2, 0)$ . Then if  $t^2 - s^2 = r^2$ , we obtain that

$$R_2 = (\pm rt, irt(r \pm t)).$$

Let  $K = \mathbb{Q}(i)$ . We found that either  $Q_2$  or  $R_2$  is in  $E(K)$  but  $P_2 = (st, st(s+t))$  is also in  $E(K)$  and  $[2]P_2 = (0, 0)$ . We can easily see that  $P_2$  and  $Q_2$  generate  $E[4] \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$  which makes  $E[4] \subset E(K)$ . This is not possible by assumption that  $E(K) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ . Hence  $\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z} \not\subset E(F)$  when  $K = \mathbb{Q}(i)$ .

Let  $K = \mathbb{Q}(\sqrt{-3})$ . Above computation shows that if  $s^2 - t^2 = \pm r^2$  for some  $r \in K$ , then  $Q_2$  or  $R_2$  is in  $E(K(i))$ . Moreover we see that the quadratic twist  $E^{-1}$  of  $E$  by  $-1$  has a point of order 4 over  $K$ . Therefore if  $E^{-1}$  has a point of order 4, then  $\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z} \subset E(F)$  and otherwise  $E(F)$  does not contain a subgroup isomorphic to  $\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ .

Let  $K = \mathbb{Q}(\sqrt{-3})$  and assume that  $E^{-1}(K)$  has a point of order 4. Then above argument shows that  $s^2 - t^2 = \pm r^2$  for some  $r \in K$ . We will show that there is no point of order 16 in  $E(F)$ . We know that there is a point  $P_3$  in  $E(F)$  such that  $[2]P_3 = P_2$ . We will show that  $P_3 \notin [2]E(F)$ . We compute

$$x(P_3) = \pm(1/2)\sqrt{\pm st}(\sqrt{s} + \sqrt{t} + \sqrt{\pm s + t})^2.$$

Assume  $P_3$  is in  $[2]E(F)$ . Then  $\sqrt{st}$  is a square in  $F$  and so  $st$  or  $-st$  is a square in  $K$ . Since  $s$  and  $t$  are relatively prime, either  $s = \pm du^2, t = \pm dv^2$  where  $d$  is a unit in  $\mathcal{O}_K$ . Only square-free units in  $\mathcal{O}_K$  are  $\{\pm\zeta_6, -\zeta_3\}$ . In

any case, we obtain a non-trivial solution to the equation  $x^4 - y^4 = z^2$  over the cyclotomic field  $\mathbb{Q}(\zeta_{12})$  which is not possible.

Now, let  $P'_2$  denote the point  $(-st, st(s-t))$  in  $E(K)$ . Then  $[2]P'_2 = (0, 0)$ . Let  $P'_3$  be in  $E(F)$  such that  $[2]P'_3 = P'_2$ . We compute

$$\begin{aligned} x(P'_3) &= -st - t\sqrt{s}\sqrt{s-t} + s\sqrt{-t}\sqrt{s-t} + (s-t)\sqrt{-ts} \\ &= \sqrt{-st}(\sqrt{s} + \sqrt{-t} + \sqrt{s-t})^2 \end{aligned} \quad (1)$$

Assume  $P'_3 \in [2]E(F)$ . Then  $\pm st$  is a square in  $K$  as before. Also  $x(P'_3) + s^2 = \sqrt{u^2 - v^2}(u + iv)(\sqrt{u^2 - v^2} + iv)$  which is also a square in  $F$ . Notice that  $x(P'_3)$  is obtained by replacing  $t$  with  $-t$  and so  $v$  replaced by  $-iv$ . Now, it is not hard to see that  $P'_3 \notin [2]E(F)$  either. Suppose now that there is a point  $P$  of order 16 in  $E(F)$ . Then  $[2]P$  can be generated by  $P_3$  and  $Q'_2$  where  $Q'_2 = P'_3 - P_3$ . Hence, for some integers  $k, l$ ,

$$[2]P = [k]P_3 + [l]Q'_2$$

Since  $[2]P$  is of order 8,  $k$  is odd. Define a point  $Q \in E(F)$  as follows:

$$Q = \begin{cases} [-(k-1)/2]P_3 - [l/2]Q'_2 & \text{if } b = 0, 2 \pmod{4} \\ [-(k-1)/2]P_3 - [(l-1)/2]Q'_2 & \text{if } b = 1, 3 \pmod{4} \end{cases}$$

Then

$$[2](P + Q) = \begin{cases} P_3 & \text{if } b = 0, 2 \pmod{4} \\ P'_3 & \text{if } b = 1, 3 \pmod{4} \end{cases}$$

This is not possible since we showed that  $P_3$  and  $P'_3$  are not in  $[2]E(F)$ . Hence  $\mathbb{Z}/16\mathbb{Z} \not\subset E(F)$  and  $E(F)_{\text{tors}} \cong \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ .  $\square$

**Proposition 10.** Let  $K = \mathbb{Q}(i)$ . If  $E(K)_{\text{tors}} \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ , then  $E(F)_{\text{tors}}$  is isomorphic to  $\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ .

*Proof.* Suppose that  $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \subset E(K)$ . Then we may assume that  $a = s^2$  and  $b = t^2$  for some  $s, t \in K$ .  $P_2 = (st, st(s+t))$  such that  $[2]P_2 = (0, 0)$ . Let  $Q_1 = (-s^2, 0)$ , then let  $Q_2$  be in  $E(K)$  such that  $[2]Q_2 = Q_1$ . Then by Lemma 9, we can compute  $x(Q_2) = s\sqrt{s^2 - t^2} - s^2$ . Since  $Q_2$  has order 4, it must be in  $E(K)$  which forces  $s^2 - t^2$  to be a square in  $K$ . Let  $r$  be in  $K$  such that

$$s^2 - t^2 = r^2.$$

Hence, we compute  $Q_2 = (sr - s^2, isr(r-s))$ . Now, by lemma 9, we know that  $\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z} \subset E(F)$ . We want to show that  $\mathbb{Z}/16\mathbb{Z} \not\subset E(F)$ . Let  $P_3$  be a point in  $E(F)$  where  $[2]P_3 = P_2$ . Then using Lemma 9, we find

$$x(P_3) = 1/2\sqrt{st}(\sqrt{s} + \sqrt{t} + \sqrt{s+t})^2.$$

Assume  $P_3$  is in  $[2]E(F)$ . Then  $st$  is a square in  $K$  by Lemma 9 and Lemma 12. Since  $s$  and  $t$  are relatively prime, either  $s$  and  $t$  are both squares or they are both  $i$  times a square. Since  $-1$  is a square, we do not have to consider  $-iu^2$ . Now, let  $u, v$  be in  $K$  such that  $s = iu^2, t = iv^2$ .

Then the equation  $s^2 - t^2 = r^2$  gives us  $-u^4 + v^4 = r^2$  which has no nontrivial solutions over  $K$ . Similarly, if  $u, v$  are both squares, then  $u^4 - v^4 = r^2$ . This proves that  $P_3 \notin [2]E(F)$ . Similarly, we can compute  $Q_3$  where  $[2]Q_3 = Q_2$ .

$$\begin{aligned} x(Q_3) + s^2 &= \sqrt{(sr - s^2)sr} + \sqrt{(sr - s^2)(sr - r^2)} + \sqrt{(sr - r^2)sr} + sr \\ &= s\sqrt{r}\sqrt{r - s} + \sqrt{sr}\sqrt{-(r - s)^2} + r\sqrt{s}\sqrt{s - r} + sr \\ &= -(-s)\sqrt{r}\sqrt{r - s} + \sqrt{r}\sqrt{-s}(r - s) + r\sqrt{-s}\sqrt{r - s} - (-s)r \\ &= \sqrt{-sr}(\sqrt{r} + \sqrt{r - s} - \sqrt{-s})^2 \end{aligned}$$

If  $Q_3$  is in  $[2]E(F)$ , then  $x(Q_3) + s^2$  is a square in  $F$ . By lemma 11,  $-sr$  is a square in  $K$ . Hence as above, either  $s, r$  are both squares or  $i$  times a square. In both cases, we obtain a non-trivial solution for the equation  $x^4 - y^4 = z^2$  which is not possible. Therefore,  $Q_3$  is not in  $[2]E(F)$ . Now, it is easy to see that  $P_3$  and  $Q_3$  generate  $E[8]$ . We will show that  $P_3 + Q_3$  in  $E(F)$  is also not in  $[2]E(F)$  and use these three points to show that there are no points of order 16 in  $E(F)$ . Let  $R_3$  be in  $E(F)$  such that  $[2]R_3 = P_2 + Q_2 = R_2$ . We find

$$x(R_3) + t^2 = (1/2)\sqrt{tr}\sqrt{i}(\sqrt{t}\sqrt{i} + \sqrt{r} + \sqrt{r + ti})^2.$$

If  $R_3$  is in  $[2]E(F)$ , then  $x(R_3) + t^2$  is a square in  $F$ . By Lemma 12,  $(tr)i$  has to be a square in  $K$ . Since  $s, t$  are relatively prime,  $t, r$  are also relatively prime. Hence, either  $t$  is a square and  $r$  is  $i$  times a square or the other way around.

We either obtain a non-trivial solution for  $x^4 - y^4 = z^2$  or  $x^4 + y^4 = z^2$ . Since they both have no non-trivial solutions over  $K$ , the point  $R_3$  is not in  $[2]E(F)$ . Now, assume there is a point  $P$  of order 16 in  $E(F)$ . Then  $2[P] = [k]P_3 + [l]R_3$  for some  $k, l \in \mathbb{Z}$ . Then, define

$$Q = \begin{cases} [(k-1)/2]P_3 + [l/2]R_3 & \text{if } k \text{ is odd, } l \text{ is even} \\ [k/2]P_3 + [(l-1)/2]R_3 & \text{if } l \text{ is odd, } k \text{ is even} \\ [(k-1)/2]P_3 + [(l+1)/2]R_3 & \text{if } k, l \text{ are both odd} \end{cases}$$

Then,  $[2]Q$  is either  $P_3, R_3$  or  $Q_3$ . It is not possible. Hence,  $\mathbb{Z}/16\mathbb{Z} \not\subset E(F)$  and  $E(F) \cong \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ . □

**Theorem 14.** Let  $K$  be the quadratic field  $\mathbb{Q}(i)$  or  $\mathbb{Q}(\sqrt{-3})$ . Assume  $E(K)_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ . Then  $E(F)_{\text{tors}}$  is isomorphic to one of the groups listed in Proposition 7, Proposition 8, Proposition 9, Proposition 10, or the group  $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ .

*Proof.* A quadratic twist of  $E$  can have torsion subgroup isomorphic to  $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ ,  $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ ,  $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ ,  $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$  or  $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ . If  $E^d(K)_{\text{tors}} \not\cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$  for some  $d \in K$ , then  $E(F)_{\text{tors}} \cong E^d(F)_{\text{tors}}$  and the latter group will be one of the groups listed in Theorem 7, Theorem 8, Theorem 9, Theorem 10.



Then we only need to analyze the case  $E^d(K) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$  for all  $d \in K$ . Now, let  $E$  be given by the equation  $y^2 = x(x+a)(x+b)$  with Mordell-Weil group  $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ . Then  $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \subset E(F)$  by Lemma 9. Let  $P_2$  be in  $E(F)$  such that  $[2]P_2 = P_1$ . Then  $P_2 = (\sqrt{ab}, \sqrt{ab}(\sqrt{a} + \sqrt{b}))$ . If  $P_3 \in [2]E(F)$ , then  $\pm ab$  is a square in  $K$ . If  $ab$  is a square, then either  $a$  and  $b$  are both squares (which implies  $P_2 \in E(K)$ ) or  $a = du^2$  and  $b = dv^2$  for some  $u, v, d \in K$ . Then  $P_2 = (uv, uv(\sqrt{d}(u+v)))$ . Therefore,  $P = (uv, uv(u+v))$  defines a point of order 4 in  $E^d(K)$  which is a contradiction to  $E^d(K)$  being isomorphic to  $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ . If  $-ab$  is a square, then  $a = -du^2, b = dv^2$ . Then we compute that  $u^2 + v^2$  has to be a square in  $K$  and  $E^d$  is isomorphic to the curve  $E' = E^d(-b, a-b)$  so it implies that  $E^d$  has a point of order 4 which is a contradiction.

If there is a point of order 8 in  $E(F)$ , then either  $\pm\sqrt{ab}, \pm\sqrt{a(a-b)} + a$  or  $\pm\sqrt{b(b-a)} + b$  is a square in  $F$ . We already showed that the first case is not possible. The other two cases follow from the  $K$ -isomorphisms

$$E : y^2 = x(x+a)(x+b) \rightarrow E' : y^2 = x(x-a)(x+b-a)$$

by sending  $(\alpha, \beta) \mapsto (\alpha+a, \beta)$  and similarly

$$E : y^2 = x(x+a)(x+b) \rightarrow E' : y^2 = x(x-b)(x+a-b)$$

sending  $(\alpha, \beta) \mapsto (\alpha+b, \beta)$ . We conclude that  $E(F) \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$  in this case.  $\square$

## 5. $E(K)_{\text{TORS}}$ IS CYCLIC

The following lemma will be useful to show that  $\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$  is not contained in  $E(F)$  when  $E(K)$  is cyclic.

**Lemma 15.** Let  $K$  be the field  $\mathbb{Q}(\sqrt{-3})$  and  $F$  be the maximal elementary abelian extension of  $K$ . Suppose  $a \in K$ . Then  $\sqrt{ai}$  can not be a square in  $F$ .

*Proof.* Suppose that  $\sqrt{ai}$  is a square in  $F$ . Then the proof of Lemma 12 shows that  $ai$  is a square in  $K(i)$ . Then

$$ai = b^2(1+i)^2 \text{ or } ai = b^2(1-i)^2 \text{ with } b \in K.$$

Then  $a = 2b^2$  or  $a = -2b^2$ . Hence  $\sqrt{ai}$  is equal to either  $b(1+i)$  or  $b(1-i)$ . In each case, we obtain that  $(1+i)$  or  $(1-i)$  are squares in  $F$ . Now let  $\beta = \sqrt{1+i}$ . Hence  $(\beta^2 - 1)^2 + 1 = 0$  and we see that  $\beta$  is a root of the polynomial

$$f(x) = x^4 - 2x^2 + 2.$$

It is not hard to see that degree of the splitting field of  $f$  is 8. If  $F$  has one root of  $f$ , then it has all of them since it is a Galois extension of  $K$ . Therefore  $F$  contains the splitting field of  $f$  and hence Galois group of  $f$  has to be an elementary abelian two group. Notice that Galois group of  $f$  is a subgroup of the permutation group on 4 letters. Since  $S_4$  does not have any transitive subgroup of order 8, we get a contradiction. Hence neither

$\sqrt{1+i}$  nor  $\sqrt{1-i}$  is a square in  $F$ . We have proved that  $\sqrt{ai}$  can not be a square in  $F$  for any  $a \in K$ .  $\square$

Let  $E : y^2 = f(x)$  be an elliptic curve with  $E(K)_{\text{tors}} \cong \mathbb{Z}/N\mathbb{Z}$ . If  $N$  is odd, then there is no point of order 2 in  $E(K)$ . Since 2-torsion points on  $E$  are  $(\alpha_i, 0)$  where  $\alpha_i$  are the roots of  $f$ ,  $E(K)_{\text{tors}}$  being odd implies  $f$  is irreducible over  $K$ . Therefore,  $f$  is irreducible over  $F$ . Then  $E(F)_{\text{tors}}$  is also odd and we analyzed this case in the first section. Hence, we assume that  $N$  is even.

**Proposition 11.** Let  $E$  be an elliptic curve over  $K$  and suppose that  $E(K)_{\text{tors}} \cong \mathbb{Z}/2N\mathbb{Z}$  for some integer  $N$ .

- If  $K = \mathbb{Q}(i)$ , then  $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \subset E(F)$  and  $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \not\subset E(F)$ .
- If  $K = \mathbb{Q}(\sqrt{-3})$ , then  $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \subset E(F)$  and  $\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z} \not\subset E(F)$ .

*Proof.* Let the elliptic curve  $E$  be given by the equation  $y^2 = f(x)$ . then  $f$  has one root over  $K$ . Wlog, we assume that  $E$  is given by  $y^2 = f(x) = x(x - \alpha)(x - \beta)$ . Since  $E$  does not have the full 2-torsion, there is a point  $Q_1 = (\alpha, 0)$  defined over a quadratic extension of  $K$  but not over  $K$ . Then we claim that  $Q_1 \notin [2]E(F)$  when  $K = \mathbb{Q}(i)$ .  $\alpha$  and  $\beta$  can be written as  $a + b\sqrt{c}$  and  $a - b\sqrt{c}$  since they are defined over  $K(\sqrt{c})$  for some  $c \in K$  and they are conjugate of each other. Then  $\alpha - \beta = 2b\sqrt{c}$ . If  $\alpha - \beta$  is a square in  $F$ , then  $c$  is a square in  $K$  which gives a contradiction. Hence  $\alpha - \beta$  is not a square in  $F$  and so  $Q_1 \notin [2]E(F)$ . Therefore,  $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \not\subset E(F)$ . We know also that  $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \subset E(F)$  since  $f$  factors into a linear term and a quadratic.

This part of the proof closely follows Fujita's proof for  $K = \mathbb{Q}$  (found in [3]) closely. Let  $K = \mathbb{Q}(\sqrt{-3})$ . If  $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \subset E(F)$ , then  $c = -1$  by the previous paragraph, and we can assume  $\alpha = a + bi$ . Let  $P_2$  be a point where  $2P_2 = (0, 0)$ . Suppose that  $E[8] \subset E(F)$ . Then  $P_2$  is in  $[2]E(F)$  which implies  $\sqrt{\alpha\bar{\alpha}}$ ,  $x(P_2) - \alpha$  and  $x(P_2) - \bar{\alpha}$  are all squares in  $F$ . Hence by Lemma 12,

$$\alpha\bar{\alpha} = a^2 + b^2 = \pm d^2$$

for some  $d$  in  $K$ . In both cases, we obtain either

$$(x(P_2) - \alpha)(x(P_2) - \bar{\alpha}) = 2d(d - a) = e^2 \quad (2)$$

or

$$(x(P_2) - \alpha)(x(P_2) - \bar{\alpha}) = 2d(d + b) = f^2 \quad (3)$$

for some  $e, f \in K$ . We can parametrize  $a, b, d$  as  $k(m^2 - n^2), 2kmn, k(m^2 + n^2)$  (or switch the order of  $k(m^2 - n^2)$  and  $2kmn$ ) for some  $k, m, n \in K$ . Now, equation (2) or (3) gives us either  $m^2 + n^2$  is a square in  $K$  or  $2(m^2 + n^2)$  is a square in  $K$ . Suppose  $2(m^2 + n^2)$  is a square in  $K$ , then  $m^2 + n^2$  is divisible by 2 and so  $m^2 - n^2$  which means that  $a, b, d$  are all divisible by 2. Notice that 2 remains as a prime in  $\mathcal{O}_K$ . In this case, we can take twist of  $E$  by 2.

Since  $E$  and  $E^2$  are isomorphic over a quadratic extension,  $E(F) \cong E^2(F)$ . Therefore it is enough to consider the case where  $a, b$  are not both divisible by 2. Hence we may suppose that  $m^2 + n^2$  is a square in  $K$ .

Then we compute  $x(Q_2)$  where  $Q_1 = [2]Q_2$ . We know that

$$x(Q_2) - \alpha = \sqrt{\alpha(\alpha - \bar{\alpha})}$$

is a square in  $F$ . Parametrizing  $m$  and  $n$  again, we see that  $\sqrt{ri}$  has to be a square in  $F$  where  $r$  is a polynomial of  $m, n$  over  $K$  but this is not possible by Lemma 15.  $\square$

**Proposition 12.** Let  $K = \mathbb{Q}(\sqrt{-3})$ . If  $E(F)$  contains a point of order 4, then for some  $d \in K$ , the quadratic twist  $E^d$  of  $E$  by  $d$  has a point of order 4 in  $E(K)$ .

*Proof.* Proof is same with the case  $K = \mathbb{Q}$  and it can be found in [3].  $\square$

**Proposition 13.** Let  $E$  be an elliptic curve over  $K = \mathbb{Q}(\sqrt{-3})$ . Then  $E(F)$  cannot have a subgroup isomorphic to  $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$ .

*Proof.* Suppose that  $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z} \subset E(F)$ . Then by Lemma 12,  $E^d(K)$  has a point of order 4 for some  $d \in K$ . Since  $E$  and  $E^d$  are quadratic twists,  $E(F) \cong E^d(F)$  and hence  $E^d(F)$  has a Galois invariant subgroup of order 20 which is not possible by Proposition 1.  $\square$

**Proposition 14.** Let  $E$  be an elliptic curve over  $K$ . Then  $E(F)$  cannot have a subgroup isomorphic to  $\mathbb{Z}/12\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$ .

*Proof.* If  $E(K)$  contains  $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ , then  $E(F)$  cannot have a subgroup isomorphic to  $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$  since we previously analyzed each case. If  $K = \mathbb{Q}(i)$ , then  $E[4]$  is not contained in  $E(F)$  by Lemma 11. Hence we assume that  $K = \mathbb{Q}(\sqrt{-3})$ . If necessary, replacing  $E$  by a twist, we may assume that  $E$  has a point  $P$  of order 3 and a  $K$ -rational subgroup of order 4 (arising from a twist). Let  $E' := E/\langle P \rangle$ . Then  $E'$  has a cyclic isogeny of order 9 defined over  $K$  since  $E$  has an additional  $K$ -rational 3-cycle. Then  $E'$  has a  $K$ -rational subgroup of order 36 which is not possible by Proposition 1. Hence there is no such curve over both fields  $\mathbb{Q}(i)$  and  $\mathbb{Q}(\sqrt{-3})$ .  $\square$

**Proposition 15.** Let  $E$  be an elliptic curve over  $K$ . Then  $E(F)$  cannot have a subgroup isomorphic to  $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/32\mathbb{Z}$ .

*Proof.* Suppose that  $E$  is an elliptic curve defined over  $K$  with  $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/32\mathbb{Z} \subset E(F)$ . Then by Lemma 12, we may assume that  $E(K)$  has a point of order 4. Let us call this point with  $P_2$ . We pick generators  $x, y$  for the 2-adic Tate module  $T_2(E)$  of  $E$  such that  $x \equiv P_2 \pmod{4}$ . Notice that  $E[4] \subset E(F)$ .

Then the 2-adic representation of the group  $\text{Gal}(\bar{F}/F)$  is given as follows:

$$\begin{aligned} & \text{Gal}(\bar{F}/F) \rightarrow \text{Aut}(T_2(E)) \\ \rho_2 : \sigma & \mapsto \begin{pmatrix} 1 + 2^2 a_\sigma & 4c_\sigma \\ 4b_\sigma & 1 + 4d_\sigma \end{pmatrix} \end{aligned} \quad (4)$$

for  $a_\sigma, b_\sigma, c_\sigma$  and  $d_\sigma$  in  $\mathbb{Z}_p$ .

Note that  $F$  contains primitive 8'th root of unity and hence

$$\det(\rho_2(\sigma)) \equiv 1 \pmod{8}$$

since  $\zeta_8^{\det(\rho_2(\sigma))} = \sigma(\zeta_8) = \zeta_8$ . Computing the determinant, we obtain that  $a_\sigma + d_\sigma \equiv 0 \pmod{2}$ . Let  $E' = E/\langle P_1 \rangle$  where  $P_1 = [2]P_2$  and  $\phi$  be the morphism  $E \rightarrow E'$ . We will choose the generators of  $T_2(E')$  as  $x'$  and  $y'$  where  $2x' = \phi(x)$  and  $y' = \phi(y)$ . Hence the 2-adic representation of  $\text{Gal}(\bar{F}/F)$  is given as:

$$\rho'_2 : \sigma \mapsto \begin{pmatrix} 1 + 2^2 a_\sigma & 8c_\sigma \\ 2b_\sigma & 1 + 4d_\sigma \end{pmatrix} \quad (5)$$

Since  $E(K)$  has a point of order 4,  $E'(K)$  contains full 2-torsion. Hence by Lemma 9, the full 4-torsion  $E[4]$  is contained in  $E(F)$ . Hence the representation in (5) tells us that  $b_\sigma$  is divisible by 2 for every  $\sigma \in \text{Gal}(\bar{F}/F)$ . Let  $b_\sigma = 2b'_\sigma$ . Also notice that  $E'(F)$  must have a point of order 16 since  $E(F)$  has a point of order 32. Let  $kx' + ly' \pmod{16}$  be such a point for some  $k, l \in \mathbb{Z}$  and at least one of  $k, l$  is not divisible by 2. Moreover this point is fixed under the action of  $\text{Gal}(\bar{F}/F)$ .

If  $a_\sigma$  is a unit in  $\mathbb{Z}_2$  for some  $\sigma$ , then so is  $d_\sigma$  since  $a_\sigma + d_\sigma \equiv 0 \pmod{2}$ . Then we obtain from the representation in (5) that

$$(1 + 4a_\sigma)k + 8c_\sigma l \equiv k \pmod{16} \quad (6)$$

$$(4b'_\sigma)k + (1 + 4d_\sigma)l \equiv l \pmod{16} \quad (7)$$

An easy computations show that  $k, l \equiv 0 \pmod{2}$  which is a contradiction. Hence  $a_\sigma \equiv 0 \pmod{2}$  for all  $\sigma \in \text{Gal}(\bar{F}/F)$  and so is  $d_\sigma$ . Notice that  $E'[8] \not\subset E'(F)$ . This can be seen from the results in the previous section where we studied the full 2-torsion case. Hence  $b'_\sigma$  is not divisible by 2 for some  $\sigma_1$ . (see the representation in (5).) Once again using equations (6) and (7), we compute that  $c_\sigma \equiv 0 \pmod{2}$  for all  $\sigma$  which implies that  $E[8]$  is contained in  $E(F)$ . However our previous computations and Lemma 11 shows that if  $E[8]$  is in  $E(F)$ , then  $E(F)$  does not contain a point of order 16. Hence we arrive at a contradiction.  $\square$

**Corollary 15.1.** Let  $E : y^2 = x(x+a)(x+b)$  be an elliptic curve defined over  $K$ . Assume that  $E(K)_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ . Then

$$E(F)_{\text{tors}} \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}.$$

*Proof.* The proof follows from the Proposition 7 and the previous proposition.  $\square$

**Proposition 16.** Let  $E/K$  be an elliptic curve. Then  $E(F)$  cannot be isomorphic to  $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ .

*Proof.* We will proceed the same way as in previous proposition. The representation of  $\text{Gal}(\bar{F}/F)$  on  $T_2(E)$  and  $T_2(E')$  is same as given in the above

proof. Since  $E'(F)$  contains full 2 torsion and also a point of order 3,  $E(F) \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$  by Proposition 8. Hence  $b_\sigma \equiv 0 \pmod{2}$  for all  $\sigma$ . If  $a_\sigma \equiv 0 \pmod{2}$  for all  $\sigma$ , then so is  $d_\sigma$  and  $y' \pmod{8}$  is stabilized under the action of  $\text{Gal}(\bar{F}/F)$ . However,  $E'(F)$  does not have a point of order 8. Hence  $a_\sigma$  is not divisible by 2 for some  $\sigma_1$ . Then similar to Proposition 15, we see that existence of a point of order 8 in  $E(F)$  is not possible.  $\square$

**Theorem 16.** Let  $K$  be a cyclotomic field and  $E$  be an elliptic curve defined over  $K$ ,  $F$  be the maximal elementary abelian extensions of  $K$ .

- Let  $K = \mathbb{Q}(i)$ . Then  $E(F)_{\text{tors}}$  is isomorphic to one of the following groups:

$$\begin{aligned} \mathbb{Z}/2N\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} & \quad (N = 2, 3, 4, 5, 6, 8) \\ \mathbb{Z}/4N\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} & \quad (N = 2, 3, 4) \\ \mathbb{Z}/N\mathbb{Z} \oplus \mathbb{Z}/N\mathbb{Z} & \quad (N = 2, 4, 6, 8) \end{aligned}$$

or  $1, \mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/5\mathbb{Z}, \mathbb{Z}/7\mathbb{Z}, \mathbb{Z}/9\mathbb{Z}, \mathbb{Z}/15\mathbb{Z}$ , and  $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ .

- If  $K = \mathbb{Q}(\sqrt{-3})$ , then  $E(F)$  is either isomorphic to one of the above groups or

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/32\mathbb{Z}$$

*Proof.* We will prove the theorem by eliminating groups from the list given in Theorem 8. Suppose that  $E(F)_2 \neq 1$ . If  $E(F)_{2'} = 1$ , then either  $\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$  is not contained in  $E(F)$  or  $E(F) \cong \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ . Then with the notation of Theorem 8, if  $b = 3$ , then  $r = 0$ . By Proposition 15, if  $b = 2$ , then  $r \leq 2$ . We obtain eight possibilities in this case.

Suppose  $E(F)_{2'} \cong \mathbb{Z}/3\mathbb{Z}$ . If  $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$  is contained in  $E(K)$ , then  $E(K) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$  and we showed that  $E(F) \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$ . Otherwise, we know that  $E(F)$  cannot contain  $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$  if  $K = \mathbb{Q}(i)$ . Similarly  $E(F)$  cannot contain  $\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$  if  $K = \mathbb{Q}(\sqrt{-3})$ . Along with Proposition 16, we are left with three possible groups.

The case  $E(F)_{2'} \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$  follows from Lemma 14, Proposition 11 and Theorem 8. The only possible group is  $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ . Similarly when  $E(F)_{2'} \cong \mathbb{Z}/5\mathbb{Z}$ , it follows from Proposition 11, Lemma 13 and Theorem 8 that the only option is  $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$ . The case where  $E(F)_2 = 1$  was done in the first section. Hence the result follows.  $\square$

**Remark.** Every group we listed in Theorem 16 except  $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/32\mathbb{Z}$  also appears as the torsion subgroup of some elliptic curve defined over  $\mathbb{Q}$  in its maximal elementary abelian 2 extensions. We were able to prove neither the nonexistence of an elliptic curve defined over  $\mathbb{Q}(\sqrt{-3})$  with such a subgroup in  $E(F)$  nor give an example of such a curve.

#### ACKNOWLEDGEMENTS

The author wishes to thank Sheldon Kamienny for suggesting this problem and for his kind support. Samir Siksek provided valuable insight for

a part of the proof of Theorem 2. This work also greatly benefited from conversations with Burton Newman and Jennifer Balakrishnan.

## REFERENCES

- [1] G. Frey and M. Jarden, *Approximation theory and the rank of abelian varieties over large algebraic fields*, Proc. London Math. Soc. 28 (1978), 112128. 1
- [2] Yasutsugu Fujita, *Torsion Subgroups of Elliptic Curves with Non-cyclic Torsion over  $\mathbb{Q}$  in Elementary Abelian 2-Extensions of  $\mathbb{Q}$* , Acta Arithmetica **115**.1(2004).
- [3] Yasutsugu Fujita, *Torsion subgroups of elliptic curves in elementary abelian 2-extensions of  $\mathbb{Q}$* , Journal of Number Theory, Volume **114** (2005).
- [4] S. Kamienny, *Torsion points on elliptic curves and  $q$ -coefficients of modular forms*, Invent. Math. 109 (1992), 221229.
- [5] M. A. Kenku, F. Momose, *Torsion points on elliptic curves defined over quadratic fields*, Nagoya Math. J. 109 (1988), 125149.
- [6] M.A.Kenku, *Rational  $2^n$ -torsion points on Elliptic Curves defined over Quadratic Fields*, J.London Math. Soc.(2) **11**(1975),93-98.
- [7] Anthony W. Knap, *Elliptic curves*, Mathematical Notes, vol. 40, Princeton University Press, Princeton, NJ, 1992. MR1193029 (93j:11032)
- [8] Daniel Sion Kubert, *Universal bounds on the torsion of elliptic curves*, Compositio Math. 38 (1979), no. 1, 121128.
- [9] Laska Michael and Martin Lorenz, *Rational Points on elliptic curves over  $\mathbb{Q}$  in elementary abelian 2-extensions of  $\mathbb{Q}$* , J. Reine Angew Math., **355** (1985)
- [10] B. Mazur, *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*, Invent. Math. 44 (1978), no. 2, 129162, DOI 10.1007/BF01390348
- [11] Mordell, L. J. (Louis Joel) *Diophantine Equations*, (Pure and applied mathematics (Academic Press) v. 30)
- [12] Najman Filip, *Complete classification of torsion of elliptic curves over quadratic cyclotomic fields*, J. Number Theory 130 (2010), 1964-1968.
- [13] Najman Filip, *Torsion of rational elliptic curves over cubic fields and sporadic points on  $X_1(n)$* , Math. Res. Letters.
- [14] Burton Newman, *Growth of Torsion in Quadratic Extensions of Quadratic Cyclotomic Fields*, <http://digitallibrary.usc.edu/cdm/ref/collection/p15799coll3/id/546672>.
- [15] A.Ogg, *Rational points on certain elliptic modular curves*, A.M.S. Symposium on Analytic Number Theory and and related parts of analysis (St. Louis, 1972). Amer. Math. Soc, (1973), 221-231.
- [16] Ken Ono, *Eulers concordant forms*, Acta Arith. 78 (1996), no. 2, 101123. MR1424534 (98c:11051)
- [17] Joseph H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Math- ematics, vol. 151, Springer-Verlag, New York, 1994.
- [18] Joseph H. Silverman, *The arithmetic of elliptic curves*, Second, Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009.
- [19] Michael Stoll, *Rational Points on Curves*, arXiv:1008.1905.
- [20] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput., 24 (1997), 235265

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF SOUTHERN CALIFORNIA, LOS ANGELES, CALIFORNIA 90089

*E-mail address:* ejder@usc.edu